ITI Promoting Innovation Worldwide

December 15, 2023

Robert J. Costello
Chief Information Officer
Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Submitted via reginfo.gov
ICR REFERENCE NUMBER: 202311-1670-001
TITLE: Secure Software Self-Attestation Common Form

Response from the Information Technology Industry Council on Secure Software Self-Attestation Form

Dear Mr. Costello,

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback to the open Request for Comment on Secure Software Self-Attestation Form ('the Form'). ITI is the premier global advocate for technology, representing the world's most innovative companies. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers with the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

We value the opportunity to submit these comments as we believe that important steps need to be taken before the collection of these forms can commence. Some of the changes from the previous version address concerns that many within industry had raised. The most prominent example is the inclusion of "to the best of my knowledge" in the attestation statement. Other changes, however, negate the positive progress that has been made, exacerbate old problems, or create new ones entirely. Moreover, several critical points that industry previously raised remain unaddressed.[1] For example, we urge the government to address industry's prior concerns regarding aligning vulnerability related requirements with the Secure Software Development Framework (SSDF) by focusing on critical and high security vulnerabilities. We also encourage the government to exempt software that is developed for or at the direction of the federal government from these attestation requirements. Additionally, the government should provide guidance on when updated attestation forms are required (e.g., not requiring updates for minor administrative changes).

Going forward, to set federal agencies and software producers up for success to meet the requirements outlined in M-22-18 and M-23-16, we believe additional steps need to be taken. To that end, we recommend the government:

- Reinstate the designee option for signature,
- Align the attestation language to avoid legal ambiguity,
- Clearly define the term "provenance,"

[1] https://iticdc.sharepoint.com/:b:/s/PublicSectorInternal/EcBaCdPTaWdLhiuddGkodEIBXJB2q9WeO7y7516J2X29w?e=DwDZ9C

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

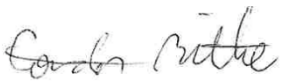
Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

- Clarify and correct the burden statement,
- Specify the collection process for software that was developed between M-22-18 and availability of final Form,
- Readjust collection timelines from M-23-16 to be contingent upon completion of agency assignments outlined in M-22-18,
- Address technical issues, and
- Host a meeting between corporate legal teams and policymakers to work out the remaining concerns.

We thank you for your consideration of our comments. To schedule a targeted follow up discussion, please contact Leopold Wildenauer, Senior Manager of Policy, at lwildenauer@itic.org.

Sincerely,



Gordon Bitko
Executive Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)

ITI's Comments:

Reinstate the Designee Option

The option for an organization to identify the most appropriate signatory must be reinstated to make this form workable for large to medium enterprises, especially those that are headquartered outside of the United States. We sympathize with the desire to raise cybersecurity considerations to the C-Suite and Board Rooms of companies. However, the decision to require this form to be signed by the Chief Executive Officer (CEO) or Chief Operating Officer (COO) of the software producer is unnecessary, unduly burdensome, and at odds with existing legal and commercial practice obligations, which allow companies to delegate signature authority to designated individuals with responsibility for such matters. First, neither M-22-18 nor M-23-16 make any mention of CEOs or COOs. This means that there is no legal directive to retain this requirement.

Secondly, this requirement is unduly burdensome for software producers as it lacks proportionality to the duties of a large enterprise CEO or COO. For large, multi-national corporations, these executives focus on setting and implementing the strategic vision of the company. They do not get involved in day-to-day business operations such as signing government contracts or aggregating supporting documentation. We ask that CISA and OMB afford software producers the right to select an appropriate position(s) to sign the Forms.

Finally, this requirement is unworkable for businesses that are not headquartered in the United States. The current phrasing puts foreign-owned companies out of compliance with 32 CFR Part

2004.34 Foreign Ownership, Control, or Influence (FOCI).[2] These companies need to have the ability to identify the best representative within their company and delegate the signature authority accordingly. It is, therefore, essential to reinstate the designee option to ensure consistency of this form with existing laws and regulations.

Align Attestation Language to Avoid Legal Ambiguity

SSDF Task RV 1.3 indicates that vendors must "have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy." However, attestation statement 4 c) requires the operation of a vulnerability disclosure program. Vulnerability disclosure programs are just one of four notional implementation examples for SSDF Task RV 1.3. Attestation Statement 4 c) should be consistent with the task level requisite and be updated to read: "The software producer has a policy that addresses vulnerability disclosure and remediation, and implements the roles, responsibilities, and processes needed to support that policy." We recommend the use of one legally sound attestation statement. Section III of the Form currently contains two attestation statements that introduce legal ambiguity through the use of inconsistent attestation language. The first states that the software producer "makes consistent use of the following practices" whereas the second states that "all requirements outlined above are consistently maintained and satisfied." This representation creates legal ambiguity and introduces significant legal risk under the False Claims Act.

To address this issue, we strongly recommend the use of the following statement which we believe is something that a company representative can attest to:

> "I hereby attest that I have a reasonable basis to conclude that the company presently and in good faith makes consistent, reasonable and risk-based use of the practices identified by the Form, subject to the separately provided plan of actions and milestones (POA&M). I further attest that the company will provide notice through the centralized repository if conformance to any element of this attestation is no longer materially valid."

Further, we appreciate that CISA and OMB moved the Minimum Attestation Reference table to an Appendix, but we reiterate our request that the "Filling out the Form" section clarify that the four attestation statements are to be read as expressly written and that the reference table is for informational purposes only and does not influence, modify, embellish, or otherwise affect the four attestation statements. Finally, we urge the government to clarify that any documentation submitted pursuant to self-attestation will remain confidential, protected from unauthorized disclosure, and be expressly subject to Exemption 4 of the Freedom of Information Act (FOIA) due to the highly sensitive, proprietary, and confidential nature of information being provided on SBOMs.

Clarify the Term "Provenance"

The Form uses the term "provenance" in Attestation Statement 3) under Section III but does not currently define the term. We recommend that the government work with industry to develop a consensus effective and workable definition for provenance. For example, the definition should clarify that "provenance" does not include origin information as that would be unworkable for most

[2] https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004/subpart-C/section-2004.34

software producers. For internal code, producers have not historically captured origin information, especially for multi-generation products. For third-party components, software producers do not have access to this information. For commercial third-party components, software producers have not previously required and collected origin information. For open-source software, this information may be even more difficult to collect as the code base may have multiple origins. Further, open-source maintainers rarely capture everything that is listed in the SSDF definition. We believe that these unique open-source software (OSS) provenance challenges can be resolved by extending the exclusion of OSS procured directly by the government to all OSS. Additionally, we recommend that SBOMs should be considered sufficient "provenance data" if they meet the "Depth" requirement from the National Telecommunications and Information Administration (NTIA) Minimum Elements for an SBOM, which covers "[a]t a minimum, all top-level dependencies."

Software Bills of Materials (SBOMs)

The intended end use and desired SBOM generation frequency remain unclear in the context of this form. SBOMs can be helpful for a variety of use cases, including license compliance, vulnerability scanning, asset inventory of software, artifact discovery, and the uncovering of stale dependencies. Still, it is important to remember that SBOMs are just one tool in a much larger ecosystem. We worry that SBOMs will become a "check the box" exercise with potential False Claims Act implications. While the document requires SBOMs to be produced in the NTIA-developed format, it remains silent on what risk evaluation factor agencies will apply to make this request determination. If the final version of the Form retains the mention of SBOMs, we believe it should provide parameters as to when and for what purpose an agency could or should request SBOMs to encourage consistency, efficiency, and compliance. Additionally, agencies should be required to provide assurances that contractor information will be appropriately protected.

Clarify and Correct the Burden Statement

Regarding the burden statement, there appears to be a fundamental mismatch of stakeholder expectations of the time that is required to complete the Form. The burden statement explicitly states that the "time for reviewing instructions, searching data sources, gathering, and maintaining the data needed, and the completing and reviewing of the collected information." ITI members take this form very seriously to ensure the accuracy of the information provided to the federal government. Based on internal burden estimates, ITI members have provided a range of estimates on the true compliance burden associated with this form. On the lower end, ITI members estimate the compliance burden to be around 300 full-time equivalent (FTE) hours. On the upper end, ITI members estimate that discovery alone will take 300 FTE hours with the total amounting to a little over 2000 FTE hours, or the equivalent of nearly 52 weeks of one FTE working 40hours/week. In any case, if CISA and OMB genuinely estimate this burden to be three hours and 20 minutes, then there is a drastic mismatch of expectations between the intent behind this form and the rigor that companies apply to securing their software development processes. We recommend that OMB and CISA resolve this issue either by clarifying its expectations for the completion of this form and why the estimate is so minimal, or by adjusting the burden statement to a more accurate reflection of the burden that this form inflicts upon software producers.

Specify the Collection Process for Software that was Developed between M-22-18 and the Availability of the Final Form

The requirement to collect retroactive attestation statements poses legal challenges for software that was developed between the publication of M-22-18 and the availability of the final Form. If the Form is not finalized until 2024, software producers could not have compared their software development processes against the final attestation statements in late 2022. More importantly, the scope of requirements comprising the basis for the attestation has evolved in subsequent releases of the Form. For example, the government should remove the new Form's reference to the NIST Software Supply Chain Security Guidance. It is much too late in the process to be adding potentially new and material obligations for producers, and will be impossible for vendors to retroactively attest to these new requirements issued after September 14, 2022. These changes also potentially bring other software into scope that may not have been covered by the requirements previously.

By maintaining the effective date of September 14, 2022, the Form is forcing software producers to attest to processes that were in effect at a time when the final requirements were not yet available. This issue needs to be resolved as it poses legal ambiguity. We recommend providing more clarity around how agencies should handle software that was developed during the time window between September 14, 2022, and the availability of the final requirements. Ideally, OMB would update the effective date to 90 days after the availability of the final self-attestation Form.

Readjust Collection Timelines from M-23-16 to Be Contingent upon Completion of Agency Assignments Outlined in M-22-18

The collection process will only be successful if agencies complete their prerequisite assignments that were outlined in M-22-18, specifically the inventorying of covered software and the establishment of the centralized repository. Software producers continue to grapple with understanding which of their products will be covered by the attestation requirement. Unless the software producer sold a product directly to an agency customer, producers have no way of telling which of their products are being used by any given federal agency. We have highlighted this point before, and it remains a critical issue for all products that are being sold through resellers or for software that is embedded within other commercial products like cars, screens, phones, HVAC systems, or microwave ovens. M-22-18 tasked agencies with the development of a comprehensive list of the software products in use to ensure that attestations are available on time for all products that are being used by federal agencies.

ITI member companies have reported that they were approached by some agencies that had determined that a specific product qualifies as critical software. Other agencies use the exact same software product but have not contacted the producer. This suggests that the current process is broken and that one of three things is happening:

- Agencies are at different stages of taking inventory of their products, which suggests that they are delinquent on key deliverables in M-22-18,[3]

[3] A recent report by the U.S. Government Accountability Office (GAO) observed a similar pattern. The report concluded that 20 of the 23 studied agencies had not met the requirements for investigation and remediation (event logging) capabilities pursuant to EO 14028, OMB M-21-31, and OMB M-23-03. Report available at: https://www.gao.gov/products/gao-24-105658

- All agencies have finalized their inventory and arrived at the exact same categorization of products, but take different approaches to communicating this information to the software producers; and
- Agencies interpret the critical software definition differently.

In any case, or combination of cases, OMB needs to hold agencies accountable to deliver on their assigned taskings and communicate to software producers the full inventories for critical and all other covered software. Without knowledge of the exact list of products that are covered, software producers are left guessing, which is bound to yield an inaccurate list of software products.

The other prerequisite that is critical to the timely collection of attestation statements is the availability of the centralized repository. This is critical for software producers who need assurances that their submitted data will be managed, organized, and protected in an appropriate manner that is commensurate with the level of sensitivity of information contained in supporting documentation like third party assessment packages, plans of actions and milestones (POA&Ms), and software bills of materials (SBOMs).

In a meeting with representatives from one of the responsible agencies, ITI was told that work on the centralized repository has not yet begun. We were told that the Form needs to be finalized before the work can commence. This effectively leaves only three months to get the centralized repository up and running between the publication of the final Form and the time at which agencies are required to collect the attestation forms for critical software (per M-23-16). If accurate, this seems like an impossible task to accomplish. Without the centralized repository, software producers will have none of the necessary security assurances for the protection of their submitted information, including supporting documentation like POA&Ms, SBOMs, or 3PAO assessments. This is highly concerning and introduces more risk than is mitigated by the adoption of secure software practices that software producers will need to attest to. We implore OMB to address this issue through the issuance of an update to M-23-16 that ties the start date of collecting these forms to the availability of the secure centralized repository rather than the availability of the Form.

Address Technical Issues

The Online Form Instructions do not allow for PDF uploads.[4] This requires the CEO to not only receive, evaluate, and approve the supporting documentation, but also manually complete a form in the online portal, which presents a disproportionate drain on resources. The alternative is to submit a local PDF via e-mail which may not be appropriately secure to transmit the supporting artifacts like POA&Ms or third-party assessment packages.

Additionally, there are a few critical technical issues that need to be addressed. First, the naming convention on Page 3 will not work correctly if the Form is completed at the company-wide level or for multiple products. Secondly, the version number references do not work for software as a service products or other products that do not have version numbers and receive very frequent updates. Third, the signature block should include a field for the name of the signatory as this may not be evident based on the (electronic) signature alone.

[4] See page 3 of the Form.

Host a Meeting between Corporate Legal Teams and Policymakers to Work out the Remaining Concerns

As discussed above, there are outstanding critical issues that will prevent the successful implementation of this form. We urge OMB and CISA to organize a public-private working session with an appropriate mix of corporate legal teams from software producers of different sizes, geographies, and business models. This will help ensure that outstanding issues are resolved, legal risk is mitigated, and expectations are aligned across stakeholder groups.